PCT/EP 0 0 / 0 6 3 8 7

BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

03. Aug. 2000

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

EP 00/06387

Aktenzeichen:	199 35 285.2
Anmeldetag:	27. Juli 1999
Anmelder/Inhaber:	Deutsche Telekom AG, Bonn/DE
Bezeichnung:	Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren
IPC:	H 04 L 9/20

EV

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Anmeldung.

München, den 06. Juli 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Bleidelmeier

A 9161 pat
03/00
EDV-L

Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren

Die Erfindung betrifft ein Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssel sowie ein öffentlicher Schlüssel mittels eines vorgegebenen deterministischen Verfahrens aus einer großen Zufallszahl (Seed) erzeugt wird.

Zur Sicherung von Kommunikationsdaten und gespeicherten Daten wird immer häufiger die kryptographische Technik der Verschlüsselung eingesetzt. Dabei werden die Daten unter der Kontrolle eines kryptographischen Schlüssels chiffriert. Die Daten können mit demselben Schlüssel auch wieder dechiffriert werden. Marktfähige Produkte und Softwarebibliotheken dazu stehen zur Verfügung.

Meist wird zur Verschlüsselung ein sogenanntes hybrides Verfahren eingesetzt. Bei diesen Verfahren wird die eigentliche Nachricht mit einem zufällig gewählten symmetrischen Schlüssel (Session-Key) und einem vorgegebenen symmetrischen Verschlüsselungsverfahren (z.B. DES, IDEA) verschlüsselt. Der Session-Key wird jeweils mit dem öffentlichen Schlüssel des Empfängers (es sind mehrere Empfänger möglich) und einem vorgegebenen asymmetrischen oder Public-Key-Verfahren (z.B. RSA, ElGamal) verschlüsselt. Für jeden Empfänger wird der so verschlüsselte Session-Key

...

der verschlüsselten Nachricht beigefügt. Eine Beschreibung dieser Vorgehensweise und der verwendeten Algorithmen findet man z.B. in William Stallings: "Cryptografy and Network Security: Principles and Practice", Prentice Hall, Upper Saddle River, New Jersey, 1998.

Um eine empfangene Nachricht zu entschlüsseln, muß der Empfänger zunächst mit seinem, zu seinem öffentlichen Schlüssel gehörenden, privaten Schlüssel und dem vorgegebenen Public-Key-Algorithmus den Session-Key entschlüsseln und dann mit diesem Session-Key die Nachricht entschlüsseln.

Neben der Verschlüsselung von Nachrichten werden kryptographische Verfahren auch zur Verschlüsselung gespeicherter Daten, z.B. auf dem eigenen Personalcomputer, eingesetzt. Auch hier setzt man in der Regel ein hybrides Verfahren ein, bei dem der Nutzer die Daten zunächst mit einem zufällig gewählten symmetrischen Schlüssel (Session-Key) und einem vorgegebenen symmetrischen Verschlüsselungsverfahren (z.B. DES, IDEA) verschlüsselt. Der Session-Key wird dann wiederum mit dem öffentlichen Schlüssel des Nutzers und einem vorgegebenen asymmetrischen oder Public-Key-Verfahren (z.B. RSA, ElGamal) verschlüsselt.

Der Benutzer entschlüsselt zunächst mit seinem, zu seinem öffentlichen Schlüssel gehörenden, privaten Schlüssel und dem vorgegebenen Public-Key-Algorithmus den Session-Key und dann mit diesem Session-Key die gespeicherten Daten.

Der jeweils private Schlüssel des Benutzers bzw. des Empfängers ist im folgenden mit dem Begriff Chiffrierschlüssel bezeichnet.

...

Der Chiffrierschlüssel wird entweder auf einer Chipkarte gespeichert, wobei der Zugriff auf die Chipkarte durch eine nur dem Benutzer bekannte Geheimzahl (PIN) geschützt ist, oder er wird auf einem anderen Speichermedium (z.B. Festplatte oder Diskette) gespeichert, wobei er durch ein möglichst langes Paßwort geschützt wird.

Der Chiffrierschlüssel kann verloren gehen. Wenn beispielsweise das Speichermedium zerstört wurde, auf dem er sich befand, oder wenn der Nutzer die PIN oder das Paßwort vergessen hat, mit dem der Chiffrierschlüssel gesichert war, ist ein Zugriff auf chiffrierte Daten damit nicht mehr möglich.

Um bei einem Verlust des Chiffrierschlüssels chiffrierte Daten wieder zugänglich machen zu können, sind Mechanismen notwendig, um den Chiffrierschlüssel auf sichere Weise regenerieren zu können. Zu diesem Zweck wird heute in der Regel der Chiffrierschlüssel an einer zentralen Vertrauensstelle erzeugt und sicher aufbewahrt. Die Erzeugung des Chiffrierschlüssels erfolgt in der Regel dadurch, daß zunächst mit einem statistisch guten Zufallsprozeß eine große Zufallszahl (Seed) erzeugt wird. Aus dieser Zufallszahl wird dann mit Hilfe eines deterministischen Verfahrens das Schlüsselpaar öffentlicher Schlüssel/privater Schlüssel erzeugt. Der Seed wird anschließend gelöscht. Der Nutzer erhält eine Kopie seines Chiffrierschlüssels zur Benutzung zugestellt.

Der Nutzer hat dabei keinen Einfluß auf die Erzeugung und Aufbewahrung seines Chiffrierschlüssels. Ferner ist es aufwendig, den erzeugten Chiffrierschlüssel sicher zum Nutzer zu transportieren. Als Transportmedium dient heutzutage beispielsweise die oben erwähnte Chipkarte, die dem Nutzer zugesendet wird. Auch ist ein Mißbrauch des gespeicherten Schlüssels durch die Vertrauensstelle oder ein

...

Bekanntwerden des eigenen Schlüssels durch eine Fehlfunktion der Vertrauensstelle bei der beschriebenen Vorgehensweise nicht auszuschließen.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren der eingangs genannten Art anzugeben, welches die oben angeführten Probleme löst. Insbesondere soll das Verfahren dem Benutzer allein die Entscheidung überlassen, ob ein Schlüssel wiederhergestellt werden soll.

Dem zur Lösung der Aufgabe hier vorgeschlagenen Verfahren liegt der Gedanke zugrunde, daß eine Hinterlegung des Chiffrierschlüssels zu Sicherungszwecken bei der Vertrauensstelle entfallen kann, wenn der Seed (S) nur nutzerseitig durch Hinzuziehung von nur dem Nutzer bekannten Größen (u) erzeugt wird, daß eine zur Regenerierung des Seeds geeignete Regenerierinformation (R), aus welcher der Seed von der Vertrauensstelle durch Verknüpfung mit nur ihr bekannten Informationen (v) deterministisch ableitbar ist, nutzerseitig erzeugt und verlustsicher aufbewahrt wird und daß im Falle eines Verlustes des Chiffrierschlüssels (C) durch Verknüpfung der Regenerierinformation (R) mit den geheimen Informationen (v) der Seed (S) seitens der Vertrauensstelle wieder hergestellt wird.

Dies kann bei einer ersten Ausgestaltung der Erfindung dadurch verwirklicht werden, daß eine mathematische Abbildung (Schlüsselvereinbarungsabbildung) k: $k(x,y)=z$ vorgesehen ist, für die gilt:

a) $k(k(u,v),w) = k(k(u,w),v)$ für alle u,v,w,
b) aus der Kenntnis von u und $k(u,v)$ kann in der Praxis nicht auf v geschlossen werden,
c) aus der Kenntnis von u, $k(u,v)$ und $k(u,w)$ kann in der Praxis nicht auf $k(k(u,w),v)$ geschlossen werden,

daß ein der Vertrauensstelle bekannter öffentlicher Parameter g und ein seitens der Vertrauensstelle vorhandener

...

geheimer Schlüssel v zu einem öffentlichen Schlüssel V=k(g,v) der Vertrauensstelle verknüpft sind,
daß der öffentliche Schlüssel V und eine nutzerseitig gewählte Zufallszahl u nutzerseitig zu dem Seed S=k(V,u) verknüpft werden,
daß aus dem Seed S nutzerseitig durch das vorgegebene deterministische Verfahren das Schlüsselpaar aus Chiffrierschlüssel C und öffentlichem Nutzerschlüssel U abgeleitet wird und
daß zur Ermöglichung der Wiederherstellung dieses Schlüsselpaares U und C die Regenerierinformation R=k(g,u) nutzerseitig erzeugt und verlustsicher aufbewahrt wird.

Die Zufallszahl u und der Seed S sollen nach der Erzeugung der Regenerierinformation R zur Sicherheit wieder vernichtet werden. Die Erzeugung der Regenerierinformation R erfolgt unter abhörsicheren Bedingungen, beispielsweise innerhalb des nutzerseitigen Computerterminals, so daß weder die Zufallszahl u, noch der Seed S an die Öffentlichkeit gelangen können. Die Regenerierinformation R allein ist ohne Kenntnis des geheimen Schlüssels v zur Dechiffrierung von Nachrichten und Daten ungeeignet und muß daher nicht geheim gehalten werden.

Die Regenerierinformation R kann an beliebigem Ort (beispielsweise auf Papier) aufbewahrt und im Bedarfsfall auf beliebigem, abhörbarem Wege (Post, E-Mail, WWW, ftp ...) zu der Vertrauensstelle gesendet werden.

Beispiele für geeignete Schlüsselvereinbarungsabbildungen k sind bekannt aus der Zahlentheorie. Beispielsweise kann vorgesehen sein, daß die Schlüsselvereinbarungsabbildung k eine diskrete Exponentialfunktion modulo einer großen Primzahl p: $k(x,y) := x^y$ modulo p ist und daß der öffentliche Parameter g ein Element eines mathematischen Körpers GF(p) von großer multiplikativer Ordnung ist, oder

...

daß die Schlüsselvereinbarungsabbildung k die Multiplikation auf einer elliptischen Kurve ist. Die Größenordnung der verwendeten Zahlen ist in der Praxis so zu wählen, daß es auch unter Aufbietung moderner technischer Mittel nicht möglich ist, den Wert y aus den Werten x und k(x,y) zu errechnen, was unter Voraussetzung heutiger Dechiffriertechnik bei Größenordnungen der verwendeten Primzahlen zwischen 500 und 1000 Bit gewährleistet ist.

Eine Beschreibung derartiger Funktionen findet man in William Stallings: "Cryptografy and Network Security: Principles and Practice", Prentice Hall, Upper Saddle River, New Jersey, 1998. Die vorliegende Erfindung benutzt das Prinzip des Diffie-Hellman-Schlüsselaustausches, der ebenfalls in dem genannten Werk beschrieben wird. Bei dem erfindungsgemäßen Verfahren wird aber, wie oben beschrieben, eine Vertrauensstelle vorausgesetzt, die bei Bedarf den Chiffrierschlüssel C mit Hilfe der Regenerierinformation R wieder herstellen kann.

Es kann zur weiteren Ausgestaltung der Erfindung vorgesehen sein, daß zur Wiederherstellung des Chiffrierschlüssels C im Verlustfalle seitens der Vertrauensstelle aus der Regenerierinformation R der Seed S=k(R,v) berechnet wird. Aus dem so rekonstruierten Seed S ist dann über das deterministische Verfahren der verlorene Chiffrierschlüssel C selbst berechenbar.

Aufgrund der Eigenschaft der verwendeten Abbildung k gilt $k(R,v) = k(k(g,u),v) = k(k(g,v),u) = k(V,u) = S$, was tatsächlich wieder dem ursprünglichen Seed S entspricht. Da der Vertrauensstelle das deterministische Verfahren ebenfalls bekannt ist, kann der Chiffrierschlüssel C mit Hilfe der Regenerierinformation R sehr leicht von der Vertrauensstelle auch ohne Kenntnis der Zufallszahl u wieder hergestellt werden. Der regenerierte Chiffrierschlüssel C

...

muß dem Nutzer dann auf abhörsicherem Wege zugestellt werden.

Um einem Mißbrauch des erfindungsgemäßen Verfahrens zur Erlangung fremder privater Chiffrierschlüssel C vorzubeugen, kann ferner vorgesehen sein, daß die Vertrauensstelle nach Berechnung des Seeds S und nach Ableitung des neuen öffentlichen Nutzerschlüssels U des Nutzers und des neuen Chiffrierschlüssels C aufgrund eines Schlüsselverlustes überprüft, ob der neu berechnete öffentliche Schlüssel U mit dem ursprünglichen öffentlichen Schlüssel U des Nutzers identisch ist, und den rekonstruierten Chiffrierschlüssel C nur dann an den Nutzer aushändigt, wenn dies zutrifft. Ein Verfahren zur sicheren Verknüpfung der Identität des Nutzers mit seinem öffentlichen Schlüssel U ist aus dem ITU-Standard X.509 bekannt.

In einer weiteren Ausprägung des Verfahrens ist vorgesehen, daß es mehrere Vertrauensstellen gibt, welche die Schlüsselvereinbarungsabbildung k und den öffentlichen Parameter g benutzen. Bei der Generierung des Chiffrierschlüssels C werden eine oder mehrere dieser Vertrauensstellen ausgewählt, wobei mit Hilfe jeder der ausgewählten Vertrauensstellen ein anderer Teilwert Sv des Seeds nutzerseitig wie beschrieben erstellt und die Teilseeds Sv nutzerseitig zu dem Seed S verknüpft werden. Zur Regenerierung des Chiffrierschlüssels C im Verlustfalle wird von den ausgewählten Vertrauensstellen ihr jeweiliger Teilwert Sv des Seeds S mittels der Regenerierinformation R berechnet. Die rekonstruierten Teilwerte Sv werden zur Rekonstruktion des Chiffrierschlüssels C miteinander zu dem Seed S verknüpft. Diese Vorgehensweise kann den Mißbrauch des Verfahrens durch eine Vertrauensstelle verhindern, da jede Vertrauensstelle nur einen für sich allein unbrauchbaren Teilseed Sv erstellen kann.

...

In einer weiteren Ausprägung des Verfahrens ist vorgesehen, daß die verschiedenen Vertrauensstellen verschiedene Funktionen kv oder/und verschiedene öffentliche Parameter gv benutzen und daß für jede der ausgewählten Vertrauensstellen eine eigene Regenerierinformation Rv erstellt wird. In diesem Fall muß der Nutzer für jede Vertrauensstelle das erfindungsgemäße Verfahren durchführen, und von jeder Vertrauensstelle muß ihr jeweiliger Teilseed Sv mit ihrer spezifischen Regenerierinformation Rv erzeugt werden.

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 ein Ablaufdiagramm der Erzeugung eines nutzereigenen Schlüsselpaares und

Fig. 2 ein Ablaufdiagramm der Rekonstruktion des Chiffrierschlüssels nach Verlust.

Gleiche Teile sind in den Figuren mit gleichen Bezugszeichen versehen.

Fig. 1 zeigt ein zeitliches Ablaufdiagramm der Vorgänge, die zur Erzeugung eines rekonstruierbaren nutzerspezifischen Chiffrierschlüssels C und eines öffentlichen Nutzerschlüssels U nach dem erfindungsgemäßen Verfahren notwendig sind. In der mit N bezeichneten Spalte sind von oben nach unten die nacheinander auftretenden nutzerseitigen Daten aufgeführt. Ü bezeichnet die Datenübertragungsstrecke zu einer Vertrauensstelle V. Die Vertrauensstelle V und der Nutzer N verfügen über den öffentlichen Parameter g und die große Primzahl p. Von der Vertrauensstelle V wird der öffentliche Schlüssel $V = g^v$ modulo p erzeugt und auf einfachem Wege zum Nutzer N übertragen. Der Nutzer erzeugt daraufhin mit einer von ihm gewählten Zufallszahl u einen

...

Seed S und eine Regenerierinformation R und löscht die Zufallszahl u aus Sicherheitsgründen wieder. Die Regenerierinformation G wird an die Vertrauensstelle V übermittelt. Aus dem Seed S wird durch Anwendung eines vorgegebenen und dem Nutzer und der Vertrauensstelle bekannten deterministischen Verfahrens ein öffentlicher Nutzerschlüssel U sowie ein privater, ebenfalls nutzerspezifischer Chiffrierschlüssel C erzeugt. Der Chiffrierschlüssel C dient hier zum Entschlüsseln von Nachrichten oder Daten des Nutzers.

Im Falle eines Verlustes des Chiffrierschlüssels erzeugt die Vertrauensstelle, wie in Fig. 2 gezeigt, den Seed S und den Chiffrierschlüssel C aus der vom Nutzer an die Vertrauensstelle übertragenen Regenerierinformation R durch Verknüpfung mit dem geheimen Schlüssel v neu und übermittelt ihn auf sicherem Wege an den Nutzer.

...

Ansprüche

1. Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssel sowie ein öffentlicher Schlüssel mittels eines vorgegebenen deterministischen Verfahrens aus einer großen Zufallszahl (Seed) erzeugt wird, dadurch gekennzeichnet, daß der Seed (S) nur nutzerseitig durch Hinzuziehung von nur dem Nutzer bekannten Größen (u) erzeugt wird, daß eine zur Regenerierung des Seeds geeignete Regenerierinformation (R), aus welcher der Seed von der Vertrauensstelle durch Verknüpfung mit nur ihr bekannten Informationen (v) deterministisch ableitbar ist, nutzerseitig erzeugt und verlustsicher aufbewahrt wird und daß im Falle eines Verlustes des Chiffrierschlüssels (C) durch Verknüpfung der Regenerierinformation (R) mit den geheimen Informationen (v) der Seed (S) seitens der Vertrauensstelle wieder hergestellt wird.

2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, daß eine mathematische Abbildung (Schlüsselvereinbarungsabbildung) k: k(x,y)=z vorgesehen ist, für die gilt:

a) k(k(u,v),w) = k(k(u,w),v) für alle u,v,w,
b) aus der Kenntnis von u und k(u,v) kann in der Praxis nicht auf v geschlossen werden,
c) aus der Kenntnis von u, k(u,v) und k(u,w) kann in der Praxis nicht auf k(k(u,w),v) geschlossen werden,

...

daß ein der Vertrauensstelle bekannter öffentlicher Parameter g und ein seitens der Vertrauensstelle vorhandener geheimer Schlüssel v zu einem öffentlichen Schlüssel V=k(g,v) der Vertrauensstelle verknüpft sind,
daß der öffentliche Schlüssel V und eine nutzerseitig gewählte Zufallszahl u nutzerseitig zu dem Seed S=k(V,u) verknüpft werden,
daß aus dem Seed S nutzerseitig durch das vorgegebene deterministische Verfahren das Schlüsselpaar aus Chiffrierschlüssel C und öffentlichem Nutzerschlüssel U abgeleitet wird und
daß zur Ermöglichung der Wiederherstellung dieses Schlüsselpaares U und C die Regenerierinformation R=k(g,u) nutzerseitig erzeugt und verlustsicher aufbewahrt wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Schlüsselvereinbarungsabbildung k eine diskrete Exponentialfunktion modulo einer großen Primzahl p: k(x,y) := x^y modulo p ist und daß der öffentliche Parameter g ein Element eines mathematischen Körpers GF(p) von großer multiplikativer Ordnung ist.

4. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die Schlüsselvereinbarungsabbildung k die Multiplikation auf einer elliptischen Kurve ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zur Wiederherstellung des Chiffrierschlüssels C im Verlustfalle seitens der Vertrauensstelle aus der Regenerierinformation R der Seed S=k(R,v) berechnet wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Vertrauensstelle nach Berechnung des Seeds S und nach Ableitung des neuen

...

öffentlichen Nutzerschlüssels U des Nutzers und des neuen Chiffrierschlüssels C aufgrund eines Schlüsselverlustes überprüft, ob der neu berechnete öffentliche Schlüssel U mit dem ursprünglichen öffentlichen Schlüssel U des Nutzers identisch ist, und den rekonstruierten Chiffrierschlüssel C nur dann an den Nutzer aushändigt, wenn dies zutrifft.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es mehrere Vertrauensstellen gibt, welche die Schlüsselvereinbarungsabbildung k und den öffentlichen Parameter g benutzen. Bei der Generierung des Chiffrierschlüssels C werden eine oder mehrere dieser Vertrauensstellen ausgewählt, wobei mit Hilfe jeder der ausgewählten Vertrauensstellen ein anderer Teilwert Sv des Seeds nutzerseitig wie beschrieben erstellt und die Teilseeds Sv nutzerseitig zu dem Seed S verknüpft werden. Zur Regenerierung des Chiffrierschlüssels C im Verlustfalle wird von den ausgewählten Vertrauensstellen ihr jeweiliger Teilwert Sv des Seeds S mittels der Regenerierinformation R berechnet. Die rekonstruierten Teilwerte Sv werden zur Rekonstruktion des Chiffrierschlüssels C miteinander zu dem Seed S verknüpft.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die verschiedenen Vertrauensstellen verschiedene Funktionen kv oder/und verschiedene öffentliche Parameter gv benutzen und daß für jede der ausgewählten Vertrauensstellen eine eigene Regenerierinformation Rv erstellt wird.

...

Zusammenfassung

Bei einem Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssel sowie ein öffentlicher Schlüssel mittels eines vorgegebenen deterministischen Verfahrens aus einer großen Zufallszahl (Seed) erzeugt wird, wird der Seed nur nutzerseitig durch Hinzuziehung von nur dem Nutzer bekannten Größen erzeugt. Eine zur Regenerierung des Seeds geeignete Regenerierinformation, aus welcher der Seed von der Vertrauensstelle durch Verknüpfung mit nur ihr bekannten Informationen deterministisch ableitbar ist, wird nutzerseitig erzeugt und verlustsicher aufbewahrt. Im Falle eines Verlustes des Chiffrierschlüssels wird durch Verknüpfung der Regenerierinformation mit den geheimen Informationen der Seed seitens der Vertrauensstelle wieder hergestellt.

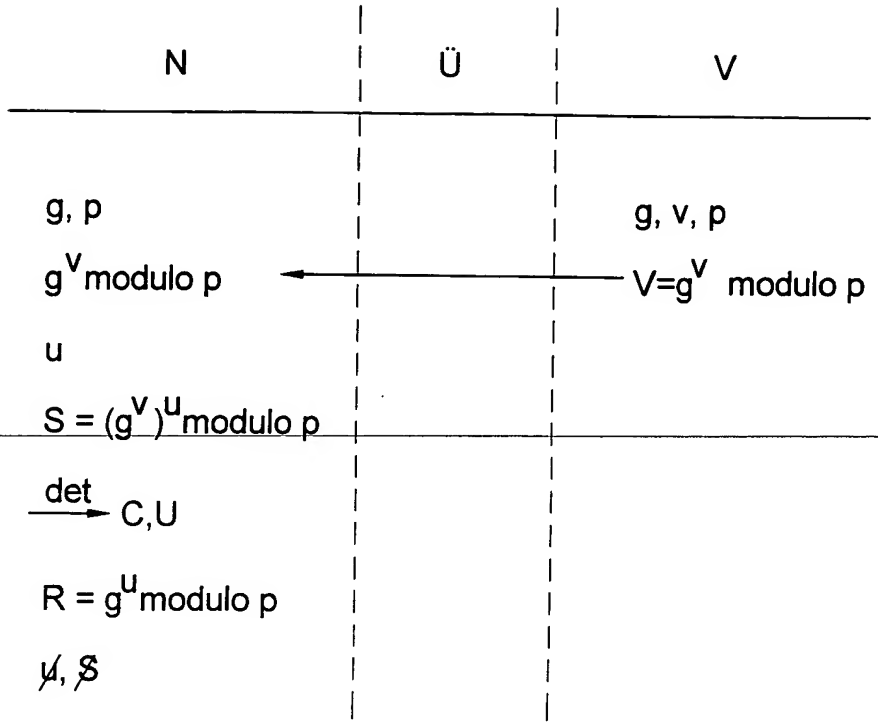
N
Ü
V
g, p
g, v, p
g^v modulo p
V=g^v modulo p
u
S = (g^v)^u modulo p
det
C,U
R = g^u modulo p
μ, S

Fig. 1

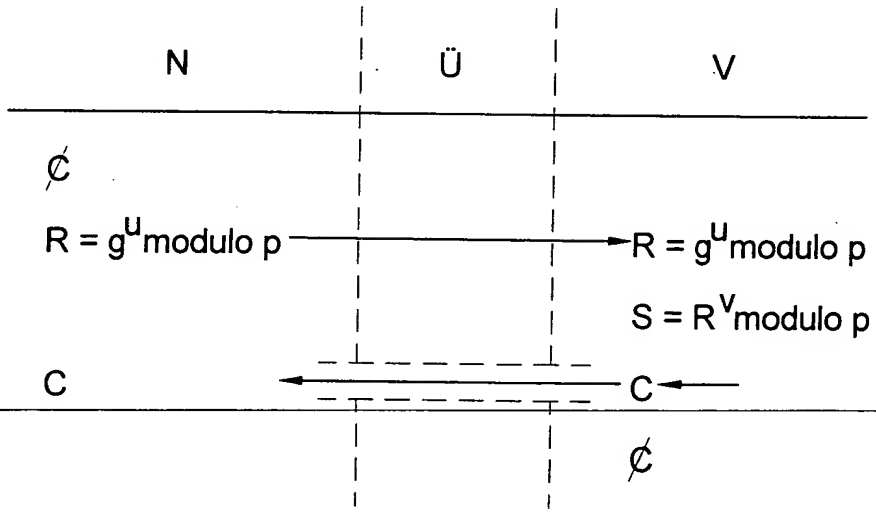
N
Ü
V
C
R = g^u modulo p
R = g^u modulo p
S = R^v modulo p
C
C
C

Fig. 2